Listing of the Claims:

The listing of the claims below replaces all previous listings of the claims.

1.   (Currently Amended) A storage system comprising:

a removable storage device configured to communication with a host device over a universal serial bus (USB), the removable storage device comprising:

a flash memory for storing at least one permission for determining access to the flash memory;

a biometric interface for receiving a request to access the flash memory;

a processor ~~for executing at least one instruction and~~ for comparing said request to said at least one permission, the comparison being independent, requiring no management by ~~without assistance from~~ an operating system of the host device, such that if said at least one permission includes a particular access type that matches the ~~of~~ access requested in said request, such access to the flash memory is provided, and alternatively if said at least one permission does not include a particular access type that matches the ~~of~~ access requested in said request, such access to the flash memory is denied; ~~not provided;~~ and

a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from said processor.

2.   (Cancelled).

3.   (Cancelled).

4.   (Previously Presented) The storage system of claim 1, wherein said biometric interface comprises:

a sample collector for collecting a biological parameter of a user.

5.   (Cancelled).

6.   (Previously Presented) The storage system of claim 4, wherein said biological parameter of the user is a fingerprint of the user.

7.   (Previously Presented) The storage system of claim 1, further comprising:
    a RAM component for storing data for performing said at least one instruction of said data processor.

8.   (Previously Presented) The storage system of claim 1, further comprising:
    a cryptographic chip for encrypting and decrypting data.

9.   (Previously Presented) The storage system of claim 8, wherein said cryptographic chip performs an authentication process.

10.   (Previously Presented) The storage system of claim 8, wherein said cryptographic chip emulates a smart card.

11.   (Previously Presented) The storage system of claim 10, wherein said cryptographic chip stores encrypted smart card data.

12.   (Previously Presented) The storage system of claim 8, wherein said cryptographic chip performs encryption immediately upon receiving a command from said processor.

13.   (Previously Presented) The storage system of claim 12, wherein said cryptographic chip creates a cryptographic signature with a hash immediately upon receiving a command from said processor.

14.   (Previously Presented) The storage system of claim 8, wherein said cryptographic chip further comprises a cryptographic chip memory for storing at least one cryptographic key and at least one cryptographic instruction for encrypting and decrypting data, such that said cryptographic chip forms a removable encryption engine.

15. (Previously Presented) The storage system of claim 14, wherein said encrypted data is stored on said cryptographic chip memory.

16. (Previously Presented) The storage system of claim 15, wherein said cryptographic chip memory is a separate flash memory device from said flash memory device.

17. (Previously Presented) The storage system of claim 15, wherein said cryptographic chip memory is said flash memory device.

18-50. (Canceled).